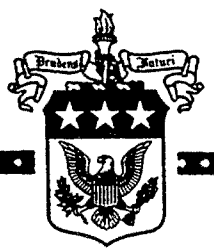
STRATEGY RESEARCH PROJECT

PROPOSED SUPPLEMENTAL GUIDANCE FOR THE DEPARTMENT OF DEFENSE'S CRITICAL INFRASTRUCTURE PROTECTION PLAN

BY

LIEUTENANT COLONEL THOMAS L. KONING
United States Army



USAWC CLASS OF 2002

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

PROPOSED SUPPLEMENTAL GUIDANCE FOR THE DEPARTMENT OF DEFENSE'S CRITICAL INFRASTRUCTURE PROTECTION PLAN

By

LIEUTENANT COLONEL THOMAS L. KONING
United States Army

Lieutenant Colonel Antulio J. Echevarria II
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Thomas L. Koning

TITLE: Proposed Supplemental Guidance for the Department of Defense's Critical Infrastructure Protection Plan

FORMAT: Strategy Research Project

DATE: 20 February 2002 PAGES: 44 CLASSIFICATION: Unclassified

This paper will argue that DoD's current policy and guidance in the area of Critical Infrastructure Protection (CIP) is not complete, and does not provide a systematic approach to accomplishing the program goals. Specifically, current guidance does not require subordinate CINCs and components to standardize and coordinate CIP planning. Because of the way DoD is structured, with the CINCs prioritizing CIP requirements along warfighting missions, and Service Components directing the budgets, CIP resource allocation decisions must be made at the DoD level. Current guidance does not provide for a feedback mechanism, so that in this time of uncertain DoD funding, our leaders can prioritize "top-down" funding allocation decisions. The current DoD CIP plan fails to provide this prioritization mechanism and therefore, our DoD leaders are not equipped to make the necessary strategic decisions. The paper recommends supplemental guidance for DoD to implement a prioritization and comparison system to justify the allocation of defense dollars to safeguard DoD operations and infrastructure from compromise or disruption. Clarification of terms and definitions, and the creation of a Critical Asset Master List (CAML) will provide "bottom-up" input in a standard manner to facilitate the DoD resource allocation feedback loop. This will allow our DoD leaders to provide timely and intelligent justification to their "top-down", funding allocation decisions. Additionally, it will ensure that the DoD CIP program goals to assure the readiness, reliability, and continuity of operations for all infrastructures supporting DoD missions are achieved.

TABLE OF CONTENTS

LIST OF ILLUSRATIONS

LIST OF TABLES

PROPOSED SUPPLEMENTAL GUIDANCE FOR THE DEPARTMENT OF DEFENSE'S CRITICAL INFRASTRUCTURE PROTECTION PLAN

> The President himself is on record as stating that Infrastructure protection is important to our economy, and to our national security, and that it will, therefore be a priority for this administration.[1]
>
> - Condoleezza Rice, June 2001

In the aftermath of the World Trade Center and Pentagon terrorist attacks, there has been much discussion of homeland security and the protection of our critical national infrastructures from attack and incapacitation. In President Bush's address to the nation on September 20, 2001, he named Pennsylvania's Governor Tom Ridge to be the new homeland security cabinet official.[2] In this capacity, Ridge will oversee the planning for the prevention of terrorist attacks to the critical infrastructure of this nation. An important piece of that infrastructure supports the Department of Defense (DoD). DoD's infrastructure is a complex and decentralized network of systems, services and processes that support the force. These systems involve private sector and government functions, which cross organizational boundaries and provide goods and services to meet defense requirements. The infrastructure is composed of functional sectors with assets that provide the operational and technical capabilities essential to military operations in peacetime and war. DoD infrastructure includes the following sectors: financial; transportation; public works; information; command, control and communications; intelligence, surveillance and reconnaissance; health affairs; personnel; emergency preparation; space and logistics.[3] It is intended that all the critical functions of DoD fall under the umbrella of one of these sectors. These assets may be owned and controlled by DoD, other U.S. governmental agencies, the foreign commercial/private sector, or host nation governments.

Unfortunately, in the area of Critical Infrastructure Protection (CIP), the national and DoD guidance is inadequate. Most certainly, the guidance could not be executed by numerous subordinates and achieve coordination across multiple sectors within DoD or across national sectors. This paper will argue that the current policy and guidance at both the national and DoD level is not complete, nor does it provide a systematic approach to accomplishing the program goals. In an effort to address this problem, the paper will provide an example of supplemental guidance for DoD to achieve coordination and prioritization for the allocation of uncertain Defense CIP funding.

HISTORICAL CONTEXT

In the spring of 1942, a small team of engineers and scientists was asked to assess the critical nodes in the German industrial complex in order to develop target lists for a strategic bombing campaign. The assessment concluded that ball bearing factories and petroleum refineries should be at the top of the targeting list. During the briefings to senior government officials, someone asked: "Are the Germans or Japanese conducting this same type of study on the US?"[4] The profound nature of this question was lost during the post-war period, but it is again at the forefront of today's national security discussions.

Although the context of the Homeland Security and CIP areas is not new, a standard definition of CIP is elusive. Current policy provides a broad definition of CIP that can serve as a baseline for discussion:

> Critical Infrastructure - are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private."[5]

The protection of critical infrastructure refers to the measures taken to eliminate or minimize the effects of a disruption so that any impact is brief, infrequent, manageable and geographically isolated.[6] This definition is not intended to include every activity in the government and private sector. A breakdown of the above list of operations provides more expansive coverage for the critical infrastructure of the nation as shown in Table 1.

OPERATION	LEAD AGENCY	RESPONSIBILITIES
Telecommunications	Commerce	Information and Communications
Energy	Energy	Electric Power; Oil and Gas Production and Storage
Banking and Finance	Treasury	Banking and Finance
Transportation	Transportation	Aviation, Highway (Trucking), Mass Transit, Pipelines, Rail, and Waterborne Commerce
Water Systems	EPA	Environmental Protection
Emergency Services	FEMA	Emergency Fire Services; Continuity of Government
Public Health	HHS	Safety of Food and the Prevention of Disease
Law Enforcement	Justice	Emergency Law Enforcement and Internal Security
Foreign Intelligence	CIA	Foreign Intelligence
Foreign Affairs	State	Foreign Affairs
National Defense	Defense	National Defense

TABLE 1. OPERATIONAL RESPONSIBILITIES

ASSUMPTIONS

To narrow the scope of this paper and provide a common basis for discussion, the following assumptions are made:

First, this paper will only address the execution of CIP within DoD. Although some of the ideas presented could apply outside of DoD, the paper will not focus on the contributions of DoD to the national CIP program or Homeland Security.

Second, that there will be funding for CIP implementation rather than an unfunded government mandate. Costs to implement CIP could be substantial if hardening of an asset is the only way to assure its availability. Although these costs could possibly be absorbed and recouped in the private sector, they cannot be absorbed in a government activity's existing budget without trade-offs.

EXISTING GUIDANCE

For DoD, there is guidance at both the national and DoD level. Policy at the highest levels of our government is by necessity general in nature. At lower levels, however, it must become more specific in order to facilitate execution.

NATIONAL POLICY AND GUIDANCE

CIP has a short history, but five key documents provide policy guidance. The initial three documents: Presidential Decision Directive (PDD) 39[7], Executive Order (EO) 13010[8] and PDD 62[9]; were an attempt by the government to scope the magnitude of the issue. Together, they identify that our national infrastructures are vulnerable, CIP is an interagency issue, and that it will require public and private partnerships to manage the vulnerabilities.[10] Neither PDD 39, EO 13010 nor PDD 62 provides any useable assessment or policy. However, they did provide the impetus, in May 1998, for PDD 63, which provides a first cut at a national policy and organizational structure

Presidential Decision Directive 63 (PDD 63), Critical Infrastructure Protection, requires the government to establish interagency working groups to coordinate the nation's requirements and responses for CIP. This manifested itself in a complex list of fifteen specific sectors (later reduced to nine)[11], four special functions, and two cross-sector activities spread across eleven agencies for action as shown in Figure 1.[12]

NATIONAL STRUCTURE FOR INFRASTRUCTURE PROTECTION

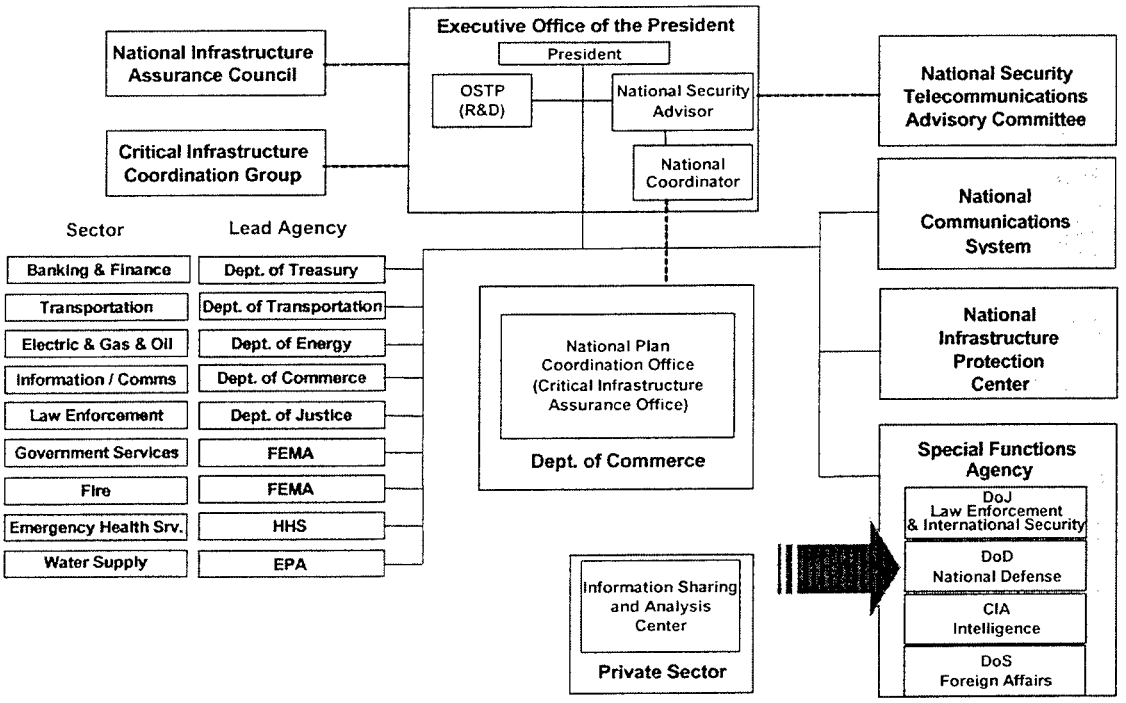


FIGURE 1. NATIONAL STRUCTURE FOR INFRASTRUCTURE PROTECTION[13]

Although unwieldy in appearance, the organization provides for eleven cabinet-rank agencies to coordinate public and private action plans within each sector. DoD is responsible for the function of National Defense. PDD 63 established the following national policy goals:

- To assure the continuity and viability of critical infrastructures.
- By June, 2003, to achieve and have the ability to protect infrastructures from intentional acts that would significantly diminish the abilities of:
  - the Federal Government to perform essential national security missions and ensure the general public health and safety;
  - state and local governments to maintain order and deliver minimum essential services; and
  - the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.
- Any interruptions must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.[14]

Subsequent policy in the National Security Strategy (NSS) does not provide better guidance. It only reiterates the goal to: "protect the ability of state and local governments to

maintain order and deliver minimum essential public services while also working with the private sector to ensure the orderly functioning of the economy and the delivery of vital services."[15]

Overall, the national guidance is inadequate. Of the five mentioned policy documents, only PDD 63 contains useful guidance in the form of policy goals and standardization of the format of subordinate policy. None of the national level documents provide any detail to guide subordinate planning activities. None of the national-level documents contain execution guidance that will allow a systematic approach to compare priorities between sectors and allocate CIP resources. At this level the policy is "broad brush", and only tells supporting agencies that they must do something in support of CIP. It is expected that each agency will develop its own CIP plan. PDD 63 allows each sector to develop its own prioritization system and criteria for the evaluation of CIP assets. National-level policy does not have to be specific, unless prioritization must be made at the national level. We expect our national leaders to allocate CIP resources against the most critical deficiencies. To do that, CIP resources cannot be allocated evenly across the sectors. The nation's most important assets must be assigned resources to address CIP deficiencies first. Therefore, a prioritization and comparison system must be established.

PDD 63 does provide some standardization across sectors by standardizing the format for CIP plans using the headings of: vulnerability assessment; remedial plan; warning; response; reconstitution; education and awareness; research and development; intelligence; international cooperation; and legislative and budgetary requirements. However, it does not provide a standardized feedback mechanism or a systematic approach to compare priorities between sectors. Without this, timely and intelligent allocation decisions cannot be justified.

DEPARTMENT OF DEFENSE POLICY AND GUIDANCE

DoD derives its CIP mission from PDD 63 in that each "special function will be responsible for coordinating all of the activities in [its] area" and "every department and agency shall develop a plan for protecting its own critical infrastructure."[16] The DoD CIP program traces its roots from DoD Directive 5160.54. Originally entitled the DoD Key Asset Protection Program (1989), it was updated as the Critical Asset Assurance Program (CAAP) in 1998. Although this document required the components to identify assets supporting both DoD and non-DoD infrastructures, conduct assessments and prioritize their importance[17] it has only been partially executed by the components.

Department of Defense Critical Infrastructure Protection Plan

At the DoD level, overall policy and guidance is found in the November 1998, Department of Defense Critical Infrastructure Protection (CIP) Plan (DoD CIP). The focus of the DoD CIP program is on the assurance of the continuity of DoD operations in the event of an infrastructure compromise or disruption. However, the DoD CIP plan does not lay out a roadmap for that assurance. Instead, the plan outlines how DoD will task organize its agencies to analyze and assess its infrastructure. The DoD CIP plan outlines the ten DoD CIP sectors and assigns an executive agent to each sector to coordinate efforts as shown in Figure 2.

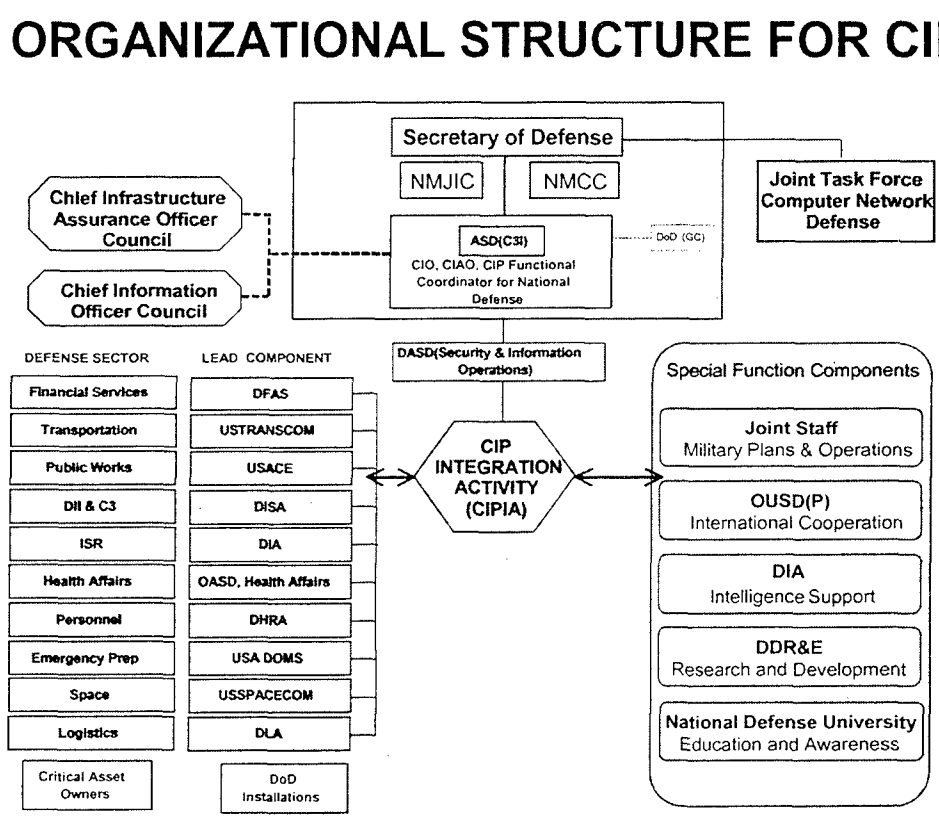


FIGURE 2. DoD ORGANIZATIONAL STRUCTURE FOR CIP[18]

Like current national policy, DoD policy does not contain a systematic approach to allow comparison of priorities between DoD sectors and/or allocate CIP resources. There would appear to be a partial correlation between the national and DoD plan sectors (Figures 1 and 2) as shown in Table 2.

Sectors where there is Correlation between the National and DoD Sectors	
National Sectors (from Figure 1)	DoD Sectors (from Figure 2)
Banking and Finance	Financial Services
Transportation	Transportation
Water Supply and Fire	Public Works
Emergency Health Services	Health Affairs
Information and Communications	DII

Sectors where there is not Correlation between the National and DoD Sectors	
National Sectors (from Figure 1)	DoD Sectors (from Figure 2)
Electric & Gas & Oil	Personnel
Law Enforcement	Emergency Preparations
Government Services	Space
	Logistics
	C3
	ISR

TABLE 2. CORRELATION BETWEEN NATIONAL AND DoD SECTORS

However, the positive correlation relationship is tenuous at best. In many cases, the DoD sector is only a small subset of the overall issue. The DoD sectors are focused on more narrowly defined defense matters rather than the national or public arenas. This is not necessarily a negative observation. Each sector has unique properties that set it apart as a sector, and the comparison of those unique properties will most likely establish each sector's CIP priorities. As long as an overarching system exists to compare different sectors the system will work.

The DoD CIP Plan is sparse on guidance. It focuses primarily on the duties of the coordination offices at the DoD-level and provides few details to the executing Lead/Executive Agents. The DoD plan does, however, state its intent, specifying that:

- Within DoD, CIP must be driven by CINC requirements (warfighting);
- That for the national defense function, DoD will focus on those cyber and physical mission critical infrastructures essential to the execution of the National Military Strategy (specifically those essential to mobilize, deploy and sustain military operations);
- CIP issues will be addressed through the existing reporting procedures: JMRR, IPL, MNS, JROC, and QDR.[19]
- In addition to identifying critical DoD owned assets; DoD will identify non-DoD owned national defense infrastructure and international defense infrastructure for inclusion;
- All DoD Sector plans will be formatted under the six major topics of: analysis and assessment; remediation; indications and warnings; mitigation; response; and reconstitution.[20]

The DoD CIP plan provides additional details to further subordinate execution. It provides guidance that warfighting requirements should drive the planning, funding, and execution of the DoD CIP effort. However, it does not provide the feedback mechanism or a systematic approach allowing comparison of priorities between sectors. Without this mechanism, DoD cannot justify the allocation of CIP resources. Additionally, DoD CIP asserts that DoD must include non-DoD assets in its critical list if required, and it more clearly defines the format of the six topic areas for each plan. However, it still fails to provide enough guidance for execution. DoD CIP implies that CINCs will prioritize DoD assets along warfighting requirements, but CINCs do not control the CIP resources in the form of service component budgets. In order to apply DoD CIP funding to the most critical assets and deficiencies first, the funding cannot be sliced out to the services on a budget percentage basis. We expect our DoD leaders to allocate CIP resources against the most critical deficiencies. Because CINCs prioritize, and Service Chiefs budget, the allocation decisions must be made at the DoD-level to ensure the warfighting priorities are protected first. Therefore, the guidance must have a feedback mechanism so assets, deficiencies, and solutions can be prioritized for resource allocation. The current DoD CIP plan fails to provide a prioritization mechanism and, therefore, our DoD leaders are not equipped to make the necessary strategic decisions.

Department of Defense Critical Infrastructure Protection Execution Plan

In March of 2000, DoD issued execution guidance as the DoD Critical Infrastructure Protection Execution Plan (DoD CIP EP). This document provides better guidance than before. Most important is that the DoD CIP EP provides criteria for components to assess their assets using a Tier system. Although not complete, the Tier system provides the first cut for the components to rank order their assets and for comparison between the sectors and components for prioritization. The Tier system is as follows:

Tier	Tier Definition
I	Warfighter suffers strategic mission failure. Specific timeframes and scenarios assist in infrastructure prioritization.
II	Sector or element suffers strategic functional failure, but warfighter strategic mission is accomplished.
III	Individual element failures, but no debilitating strategic mission or core function impacts occur.
IV	Everything else.

TABLE 3. TIER DEFINITIONS[21]

Although this is a good start, the Tier definitions do not elaborate on what is meant by "mission failure", "functional failure" or "element failures". These definitions should be rewritten to more clearly indicate the importance of the asset. The DoD CIP EP also provided more complete definitions of the critical infrastructure protection activities of: infrastructure analysis and assessment; remediation; indications and warning; mitigation; response and reconstitution. Again, this is a good start to provide some standardization across DoD, but they need additional work. The current wording and suggested improvements to these definitions will be discussed in the "Recommendations" section. Additionally, the DoD CIP EP provided a list of milestones for the components and sectors for the accomplishment of the goals set by the PDD 63.

The remaining documents in the DoD guidance do not add any additional clarification or coordination. The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3110.01C – Joint Strategic Capabilities Plan FY 2000 Interim Guidance directs that CINCs integrate CIP into all deliberate and crisis planning[22], but does not provide for any inter-CINC coordination for JCS deliberate or crisis planning. Lastly, DoD is working on a new directive, number 8590.1, entitled Critical Infrastructure Protection. Unfortunately, this new directive does not provide any additional information or missions that are not in the existing DoD CIP EP.

The bottom line is that the focus of the DoD CIP plan is to safeguard DoD operations and infrastructure from compromise or disruption. Unfortunately, the national and DoD guidance instructs us to "figure out what is critical, and protect it". This "bottom–up" approach is a good way to gather the information on critical infrastructure, but is unacceptable and unrealistic for "top-down" allocation of scarce resources. Of the ten (10) documents discussed, only three (3) provide any detail for execution: PDD 63, DoD CIP Plan and the DoD CIP Execution Plan. Together, they guide subordinate execution as follows:

- Focus on the CINC warfighting requirements - specifically those essential to mobilize, deploy and sustain military operations;
- Identify both critical DoD owned and non-DoD owned national defense infrastructure;
- Format the sector plans under the six major topics of: analysis and assessment; remediation; indications and warnings; mitigation; response; and reconstitution.
- Provide a Tier ranking system to prioritize assets.

Although useful, this guidance is still not executable. Only a clairvoyant subordinate could take this guidance and execute a plan with any chance to meet the intent of the authors of PDD 63 and DoD CIP. Most certainly, this guidance could not be executed by multiple

subordinates and achieve coordination across sectors. Subordinates need more guidance to coordinate and standardize the plan. In a time of constrained DoD funding, our leaders need a standardized and coordinated plan to compare assets for "top-down" funding allocation decisions. DoD policy does not have to be specific, unless prioritization must be made at the DoD level. Because of the way DoD is structured, with the CINCs prioritizing assets and service components directing the budgets, allocation decisions must be made at the DoD level if we expect our leaders to allocate CIP resources against the most critical deficiencies. CIP resources cannot be allocated evenly across the sectors or Components. DOD's most critical assets must have resources applied first. A prioritization and comparison system must be established that provides a standardized feedback mechanism or a systematic approach to compare priorities between sectors. Additional guidance is needed to list, prioritize, and allocate resources so we protect the most critical assets first. Without this, timely and intelligent allocation decisions cannot be justified.

DETAILED DEFINITIONS

In order to provide supplemental guidance, all agencies must use a common terminology for CIP. Defining important terms is essential. The following definitions are from the draft version of DoD Directive 8590.1 and will provide additional explanations for CIP.[23]

Assurance. Degree of confidence that a service or commodity will be available and will perform as intended when and where required.

Critical Infrastructures. Certain national infrastructures so vital that their incapacity would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures included telecommunications, electronic power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (medical, police, fire and rescue), and the continuity of government.

Critical Infrastructure Protection (CIP). The identification, assessment, and assurance of cyber and physical infrastructures that supported mission critical capabilities and requirements, to include the political, economic, technological, and information security environments essential to the execution of the National Military Strategy.

Defense Critical Infrastructures. Those systems and assets essential to mobilize, deploy, and sustain military operations in transition to post-conflict military operations, and whose loss or degradation jeopardize the ability of the Department to execute the NMS.

Infrastructure. The framework of interdependent physical and cyber-based systems comprising identifiable industries, institutions, and distribution capabilities that provides a continual flow of goods and services essential to the defense and economic security of the United States, the smooth functioning of government and all levels, or society as a whole.

Infrastructure Assurance. The surety of readiness, reliability, and continuity of operations of infrastructures such that they are (1) less vulnerable to disruption or attack; (2) harmed to a lesser degree in the event of a disruption or attack; and (3) can be reality recommended to reestablish vital capabilities.

RECOMMENDATIONS

TITLE

The program should be renamed from Critical Infrastructure "Protection" to "Assurance". CIP is not about protecting our infrastructure. The intent is to assure its continued availability under all conditions. Existing national and DOD policy appear to use the term protection and assurance interchangeably. In the strictest definition, the term assurance is an umbrella term for analysis, assessment and remediation, while protection is an umbrella term for indications, warning and response. In the loosest definition, assurance, protection and even security can be used interchangeably. Most recent DoD documents tend to define assurance as: "the state of having confidence, of being free from doubt and uncertainty; satisfaction with the truth or certainty of a matter based on an understanding of the risks;"[24] and protection as: "the state of being defended, safeguarded, or shielded from injury, loss, or destruction."[25] Assurance is the result of an effective CIP program. The goal of assurance is to have a high probability of availability and quality of specific capabilities and infrastructures. Examples of assurance activities are: dedication of physical protection resources, development of redundant capabilities/means, altering an OPLAN/CONPLAN that depends on that identified capability, or accepting risk and doing nothing.[26]

The intent is to be clear on the terminology we use. Not everything that is critical needs to be protected. Protection implies a physical or technical hardening of an asset. If there are sufficient redundancies and backups built into a particular asset, hardening options associated with the word "protection" may not be appropriate. From the definition above, the goal of the DoD CIP program is to assure the readiness, reliability, and continuity of operations for all infrastructures supporting DoD missions. In today's Defense budget, not everything that is important can have funding to protect its availability at all times. Therefore, prioritization of funding is required to assure the most critical of assets first.

A distinction should be drawn between assets that can be categorized as most critical versus those which are most vulnerable. We cannot guarantee the assurance of the continuity of everything that is important. The recommendations for improvement of the DoD CIP guidance in this paper focus on establishing a prioritization system to assure the continuity of the most critical assets first. This supports DoD's efforts to successfully execute the NMS. Those assets whose priority falls below the funding levels available will be more vulnerable to disruption. Therefore, assets that are the most vulnerable yet do not have the priority for CIP funding will remain a concern. However, if an aggressor attacks a vulnerability and fails to interrupt a critical asset, the effect of the CIP program will be achieved.

GUIDANCE

To this end, I offer the following proposals to supplement the existing DoD guidance. What I propose is an example of a course of action that was developed within the CIP Working Group at the United States Pacific Command (USPACOM) in 2001. The suggestions for improvement are listed under the headings in which the sector plans are to be formatted. The USPACOM Theater Infrastructure Protection Plan (TIPP) (DRAFT) has addressed many of the deficiencies in the national and DoD guidance. "USPACOM CIP is about mission assurance. It involves the identification, assessment, protection, and monitoring of cyber and physical mission critical infrastructures essential to the execution of the National Military Strategy. However, it is clear that the absolute protection is neither technically nor financially feasible. Therefore, as an operational readiness issue, CIP must focus on the assets most critical to the warfighter's mission to maximize the utility of protection investments."[27]

Infrastructure analysis and assessment

DoD intends that the CINC and Component CIP plans accomplish the following in the area of infrastructure analysis and assessment:

> Coordinated identification and characterization of DoD, National and International critical assets, their system and infrastructure configuration and characteristics, and the intra/interdependencies within and among infrastructure sectors; assessment of their vulnerabilities; quantification of the relationship between military plans and operations in critical assets/infrastructure; and assessment of the operational impact of infrastructure loss or compromise.[28]

Unfortunately, this intent is not completely clear as to what a CINC or Component must do. To add clarification, there are five things that should be done in infrastructure analysis and

assessment: 1) conduct a sector characterization; 2) develop the critical asset list; 3) conduct vulnerability assessments; 4) conduct interdependency analysis; and 5) prioritize the correction of the deficiencies.

First, each of the DOD sectors must independently conduct a sector characterization. A sector characterization is an analysis of all DoD and non-DoD defense assets in its area of responsibility and influence as depicted in Figure 3.

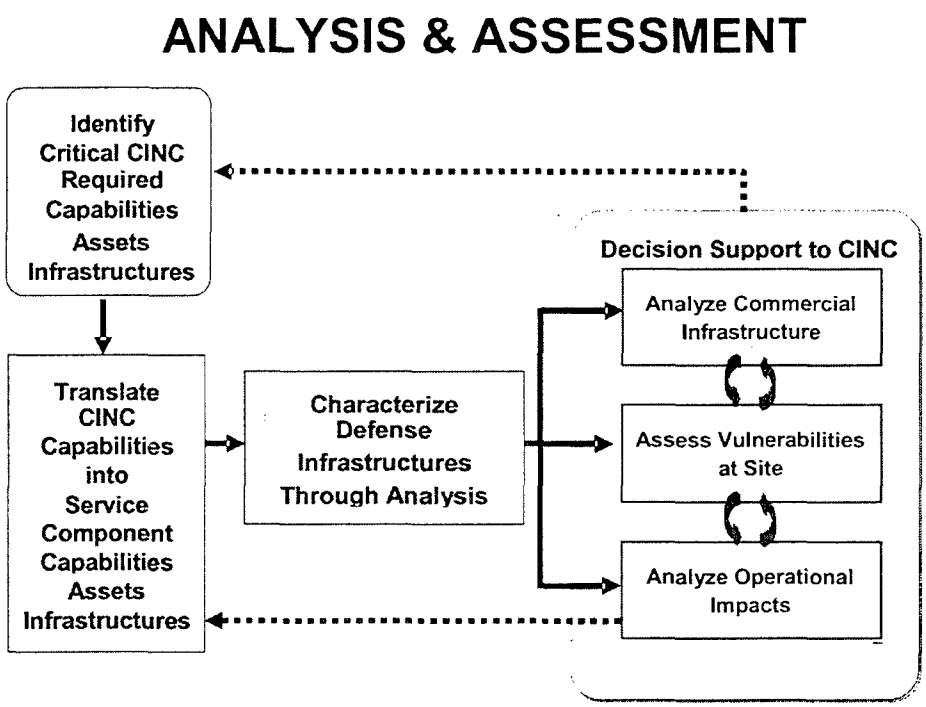


FIGURE 3. ANALYSIS AND ASSESSMENT FLOW CHART[29]

Second, this analysis needs to be in the form of a critical asset list. This critical asset list should have a standard format so that a master list can be created and the different sectors compared. Table 4 is an example of what the Critical Asset Master List (CAML) format might look like: (This example is in the format of a Word table for illustration purposes only. There are multiple database programs and formats that could be used to collect the same information.) Obviously, the number and titles of the columns can be expanded to capture additional information for risk of vulnerabilities, funding allocation, etc.

The CAML will need multiple data fields so that the information may be sorted in numerous ways. The data fields must focus the contents into useable information. Critical

	A	B	C	D	E	F	G	H	I	J
1		Asset			Location					
2	Tier	Force	System	Function	Installation	Base/Port	Facility	Common Name	Building/ Facility #	City
3	1		MILSTAR	STRATEGIC COMMS	MAKALAPA	PEARL HARBOR	PACFLT		Bldg 457	PEARL HARBOR
4	1			SPOD		PUSAN		PUSAN	Piers 4, 5, & 9	PUSAN
5	3	62nd SF Bn		Special Forces		KANEOHE MCB			Bldg 127	KANEOHE
6	3	Merchant Marine Ships	Motor Vessel	Cargo Ship			Jackson Shipping			BEAUMONT

	K	L	M	N	O	P	Q	R	S	T
1	Location			MACOM			Assessment			
2	State	Country	Coordinates	Owner	Higher HQ	Service	Assessment Type	Date	Vulnerability Type	Priority
3	HI	USA	18FAB123456	PACFLT	CINCPAC	US Navy	JSIVA	Oct 99		1
4		SOUTH KOREA	32ZTR234567	SOUTH KOREA						2
5	HI	USA	18FAB 987654	USMC	MARFORPAC	USMC				3
6	TX	USA	15DGH345678	Pacific Lines						4

Note: The data in this table is fictional. A CAML filled in with actual data would be classified as SECRET.

TABLE 4. EXAMPLE OF CRITICAL ASSET MASTER LIST

information falls in the categories of: Tier, Asset, Location, MACOM, Assessment and Priority described below:

- Tier – How important is this asset? Although volumes could be written on how to prioritize disparate assets and the definition of Tiers, nothing would cover all possibilities. Likewise, further trying to define "mission failure", "functional failure" and "element failures" would take volumes and might still not meet the requirements of a specific sector. DoD already has a mission capability rating system. Crosswalking the Tier system with C-rating systems used for the Joint Monthly Readiness Reporting (JMRR) should make the process more understandable. All services use the C-rating system for status reporting. Better definitions for the Tier system would be the inverse of the C-rating system, so that the new definition for a Tier would read, "The loss of this asset/capability would result in (inverse of C-rating definition)." Therefore, the same judgment expectations used for JMRR reporting will cover all possibilities when judging the worth and relative importance of disparate assets.

Tier	Tier Definition	Crosswalk to C-rating	C-rating Definition[30]
I	Warfighter suffers strategic mission failure. Specific time frames and scenarios assist in infrastructure prioritization.	C4	The command/agency has major deficiencies in this functional area that preclude satisfactory mission accomplishment.
II	Sector or element suffers strategic functional failure, but warfighter strategic mission is accomplished.	C3	The Service/command/agency has significant deficiencies in this functional area that prevent it from performing some portions of required missions.
III	Individual element failures, but no debilitating strategic mission or core function impacts occur.	C2	The Service/command/agency has some deficiencies in this functional area with limited impact on capability to perform required missions.
IV	Everything else.	C1	The Service/command/agency has only minor deficiencies in this functional area with negligible impact on capability to perform required missions.

TABLE 5. TIER TO C-RATING CROSSWALK

Additionally, for an asset to be given a Tier I or II rating, it must be directly linked to the execution of an OPLAN/CONPLAN or the organization's Mission Essential Task List (METL). In other words, it must be a critical capability, defined as: a capability that is central to the successful execution of an assigned OPLAN/CONPLAN/METL task. Loss or degradation of a critical capability jeopardizes the organization's ability to successfully prosecute operations in

support of the NMS. A critical capability may be made up of critical assets and/or defense critical infrastructure. Using the MILSTAR example in Table 4, the linkage to justify a Tier I ranking might be: Under multiple OPLANS and specific SIOP requirements, this CINC must have instantaneous and continuous communications with the President and/or the Secretary of Defense as provided by MILSTAR, to execute this command's mission.

- Asset – The columns of Force, System and Function all helped to identify and justify the asset. Depending on the type of asset it may fall into one or all of the mentioned categories.

- Location -- The columns of Installation, Base/Port, Facility, Common Name, Building/ Facility #, City, State, Country and Coordinates all help to identify the location of the assets.

- MACOM – The columns of Owner, Higher HQ and Service all help to identify who is responsible for the asset.

The third recommended step for completing Infrastructure Analysis and Assessment is to conduct the vulnerability assessments. The columns of Assessment Type, Date, Vulnerability Type, and Description all help to identify where initial resources must be allocated to complete the assessment requirements. A DOD-wide assessment process is under development, called the Defense Integrated Vulnerability Assessment (DIVA). When complete, it will result in evaluating an asset's vulnerability against all threats in the format of the CIP lifecycle: remediation, indications and warnings, mitigation, response and reconstitution. The following four assessments are commonly used by DoD today:

- Balanced Survivability Assessment (BSA) from the Defense Threat Reduction Agency (DTRA). This is typically used to assess an asset's ability to survive a chemical, biological, or nuclear attack.

- Special Technology Countermeasures (STC) Commercial Dependency Assessments from the Joint Program Office. This is typically used to asses the interdependencies of the DoD asset and the private sector in the areas of telecommunications; petroleum, oil and lubricants; electrical power; natural gas; transportation and municipal water supply.

- Joint Staff Integrated Vulnerability Assessment (JSIVA) from the Joint Staff Force Protection (J34). This is typically used to assess an asset's antiterrorism and force protection (AT/FP) vulnerabilities in the areas of: AT/FP structures, AT/FP procedures, building and site layout, structural engineering, blast effects and rapid response capability.

- INFOSEC Assessment Methodology (IAM) from NSA - Information Assurance (NSA-IA). This is typically used to identify and correct security weaknesses in information security systems and networks.

Fourth, once each sector has completed its asset list they must be combined into a CAML. The CAML, when sorted, will begin to show interdependencies between the sectors. For example, if the database is sorted by "location", one might determine that a particular location has a large number of high priority assets. Therefore, it might mean the entire location may need to receive a high priority for completion of vulnerability assessment or protection and assurance funding options. If the database is sorted by the "asset" column it might indicate where there is sufficient redundancy and backup, so as to not require additional allocation of funds. Or it might show where there is a lack of redundancy and backup; therefore, highlighting where a vulnerability assessment should be conducted, or protection and assurance funding be allocated. If the list is sorted by "Tier" and a Tier I or II asset has not received an assessment, it will indicate where vulnerability assessments should be conducted.

Lastly in the area of Infrastructure Analysis and Assessment is the priority for correction of the deficiency or for providing assurance. This column is associated with the Tiers, but further prioritizes the assets within a Tier for assurance by hardening or redundancy by attaching a regeneration timeline to the asset.[31]

- Priority One: resources for which the loss, theft, destruction, misuse or compromise would result in "Great Harm" to the warfighting capability of the organization. "Great Harm" is defined as: the attendant or alternate capability for this asset during mission execution is not available. An example might include the loss of a CINC's strategic communication nodes (MILSTAR) that would prevent him from communicating with the President and/or Secretary of Defense in an immediate manner. In general, an asset that is Priority One for assurance is: not currently hardened or protected as required; does not have sufficient redundancy built in; back-up systems or work-arounds are not able to, or do not have the excess capacity to, handle the extra requirements; and assuming risk is not acceptable.

- Priority Two: resources for which the loss, theft, destruction, misuse or compromise would result in "Significant Harm" to the warfighting capability of the organization. "Significant Harm" is defined as: the attendant or alternate capability for this asset during mission execution would result in a replacement delay of one (1) to five (5) days. An example might include the

loss of a major port of debarkation which would cost the CINC one (1) to five (5) days to reroute incoming passengers and cargo.

- Priority Three: resources for which the loss, theft, destruction, misuse or compromise would result in "Damage" to the warfighting capability of the organization. "Damage" is defined as: the attendant or alternate capability for this asset during mission execution would result in a replacement delay of six (6) to ninety (90) days. An example might include the loss of a low-density/high-demand Active Component unit that would require mobilization of a Reserve Component unit to replace that capability.

- Priority Four: resources for which the loss, theft, destruction, misuse or compromise would "Hinder" the warfighting capability of the organization. "Hinder" is defined as: the attendant or alternate capability for this asset during mission execution would result in a replacement delay of over ninety-one (91) days. An example could include the loss of a cargo vessel containing non-immediate sustainment supplies.

The end result is that the CAML will standardize the CIP's critical first step of Infrastructure Analysis and Assessment. The CAML will Tier the importance of the asset, fully describe the asset, and prioritize the deficiency for assurance. It will assist in providing the "bottom-up" input to the CIP resource allocation process.

Remediation

DoD intends that the CINC and Component CIP plans accomplish the following in the area of remediation:

> Deliberate preventative measures undertaken to improve the reliability, availability, and survivability of critical assets and infrastructures (e.g., emergency planning for load shedding, graceful degradation and priority restoration; increased awareness, training and education; changes in the business practices or operating procedures, asset hardening or design improvements, and system level changes such as physical diversity, deception, redundancy and backups).[32]

Although the intent is defined in terms of preventative measures, the terminology is poor. Unfortunately, the original writers of the CIP plans confused the words remediation and mitigation. Remediation means: "the act or process of remedying; something that corrects an evil."[33] This implies that the action to remediate is taken "after" an event has occurred. Mitigation means: "prevention; or the abatement or diminution of something painful, harsh,

severe, afflictive or calamitous."[34] This implies that the action comes prior to an event occurring. Mitigation is the term that should be used in future documentation for the preventative measures taken to assure an asset's availability under all conditions.

It is in this area that prioritization and funding allocation decisions can greatly impact the assurance of an asset. Assurance can manifest itself in multiple forms including hardening, redundancy of systems, and backups or work-around solutions to interruptions. Generally, but not always, cost increases as the assurance choices increase from backups and work-arounds, to redundancy, to hardening. As mentioned above in the analysis and assessment section, the priority system can assist the decision makers who might not be familiar with the asset to determine whether hardening or redundancy is the correct course of action. Additionally, the priority system will add a timeliness factor to the restoration of Priority One and Two assets.

Indications and Warnings

DoD intends that the CINC and Component CIP plans accomplish the following in the area of indications and warnings:

> Tactical indications through the implementation of sector monitoring and reporting, strategic indications through Intelligence Community support, and warning in coordination with the NIPC [National Infrastructure Protection Center] in concert with existing DoD and national capabilities.[35]

These may be related to domestic criminal activity; environmental, weather, or technical anomalies that indicate system failure and/or degradation are likely. Indications are preparatory actions or preliminary infrastructure states that signify an incident is likely, planned, or underway. If indications are present, official warnings should be issued by the organization responsible for collecting and analyzing the Indications and Warnings. Defense infrastructure sectors must develop mechanisms to define, monitor, and report infrastructure conditions.[36]

For areas and interests outside the U.S., DoD has intelligence collection assets that should assist in recognizing indications and warning of a potential threat to asset assurance. However, within the U.S. this capability is generally prohibited by EO 12333[37] and DoD Regulation 5240.1-R that restricts intelligence collection on U.S. persons. CINC and Component plans should detail the interagency links (CIA, FBI and Local Law Enforcement) for obtaining timely intelligence from additional sources whether located within or outside the U.S.

Mitigation

DoD intends that the CINC and Component CIP plans accomplish the following in the area of mitigation:

> Preplanned and coordinated reactions to infrastructure warning and/or incidents designed to reduce or minimize impacts; support and complement emergency, investigation, defense, or other crisis management response; and facilitate reconstitution.[38]

Although the intent is defined as remedial actions to be taken after/during an event, the terminology is once again poor. As discussed under the remediation section above, the original writers of the CIP plans confused the words remediation and mitigation. The term that should be used in future documentation for the preplanned measures in response to a disruption of an asset's assurance is remediation. Examples in this category are graceful service degradation, load shading, network partitioning, execution of work-around plans and relocation.[39]

Response

This refers to those actions undertaken to eliminate the cause or source of an event. DoD intends that the CINC and Component CIP plans to accomplish the following in the area of response:

> Coordinated third party (not owner/operator) emergency (e.g., medical, fire, hazardous or explicit material handling), law enforcement, investigation, defense, or other crisis management service aimed at the source or cause of the incident. Response to infrastructure incidents involving Defense infrastructure will follow one of two paths: (1) affected Components and/or the JTF-CND [Joint Task Force – Computer Network Defense][40] will defend against and respond to all cyber incidents in accordance with granted authorities and established operational procedures; or (2) affected Components will defend against and respond to all non-cyber incidents in accordance with granted authorities and established operational procedures.[41]

The intent is that CINCs and Components have continuity of operations plans (COOP) to ensure their viability in response to a disruption of a critical asset. Obviously, these actions occur after a disruption has occurred. Depending on the severity of the disruption, CINCs and Components should be prepared to assist and receive assistance as specified in the Federal Response Plan (FRP). Because the FRP is designed to assist during major incidents, this section of the CIP planning should be limited to the smaller and contained disruptions that would not trigger a response activating the FRP.

Reconstitution

DoD intends that the CINC and Component CIP plans accomplish the following in the area of reconstitution: "Owner/operator directed restoration of critical assets and infrastructure."[42]

To bring assets back to the levels of service that existed before a disruption could be the most costly and time consuming task in the entire process. This may include extended COOP missions and eventual rebuilding. Although reconstitution could be a costly and time consuming event, at least priorities have been established through the proposed Tier and Priority systems to aid the decision makers in allocating assets and funding.

The bottom line is that there are numerous improvements that DoD can undertake to make CIP planning, plans and results more useable. The terms of protection, assurance, remediation and mitigation should be used correctly. The DoD guidance should give more definition and/or format to the asset identification phase. This is the critical first step in order to make informed decisions about the criticality of assets and priority of funding for mitigation of deficiencies. In today's Defense budget, not everything that is important can have funding to protect its availability at all times. Therefore, prioritization of funding is required to assure the most critical assets first.

The above recommendations provide the detail necessary to guide subordinate planning activities. They will allow a systematic approach to compare priorities between sectors within DoD and allocate CIP resources. We must provide to both our DoD leaders and subordinates the tools to allocate CIP resources against the most critical deficiencies.

The above recommendations also provide prioritization and comparison systems to justify the allocation of defense dollars, and safeguard DoD operations and infrastructure from compromise or disruption. This "bottom–up" creation of the CAML is a good way to gather the needed information on critical infrastructure.

Additionally, the CAML Tiers and Priorities will facilitate coordination and standardization from multiple subordinates and across multiple sectors. Because of the way DoD is structured, with the CINCs prioritizing assets and Components directing the budgets, we have forced allocation decisions to be made at the DoD level because we expect our leaders to allocate CIP resources against the most critical deficiencies. DoD's most critical assets must have resources applied first.

Finally, the above recommendations establish a prioritization and comparison system that provides a standardized feedback mechanism and a systematic approach to compare

priorities between sectors. This will allow our DoD leaders to provide timely and intelligent justification to their "top-down" funding allocation decisions. This will ensure that the DoD CIP program goals to assure the readiness, reliability, and continuity of operations for all infrastructures supporting DoD missions are achieved.

Both DoD and the CINCs will benefit from the above-mentioned recommendations. For DoD, the end result will be clear priorities for funding allocations within DoD assets. Assuming DoD CIP funding is not "salami sliced" to the services, our DoD leadership will have to avoid service budget rivalries to achieve maximum benefit. Additionally, for non-DoD owned assets, DoD can focus CIP efforts both in the intra-agency/political process and with industry to effect reliability and assurance of goods and services. Likewise, the prioritization of host-nation assets, goods and services, allow the Defense Chiefs to focus their treaty, SOFA, host-nation support agreements and discussions for both peacetime and wartime reliability. A CINC would receive many of the same benefits. A CINC could direct his efforts, in priority, through both reporting channels (JMRR, IPL, NMS, JROC and QDR) and by requesting special category JCS funding such as Combating Terrorism - Readiness Initiative Funds (CBT-RIF) or CINC Initiative Funds (CIF).

Additionally, for non-DoD owned assets, a CINC can focus CIP efforts with industry contacts and within governmental (National, State and Local) circles providing the goods and services to DoD. Likewise, for CINCs with OCONUS responsibilities the prioritization of host-nation assets, goods and services, allow the CINC to focus his CIP efforts when supporting SOFA, host-nation support agreements, and mutual defense agreements for both peacetime and war.

CONCLUSION

With the current CIP plan, DoD has made an effort to provide procedures for attempting to assure availability of DoD critical defense infrastructure. In its current form, the plan does not provide a good means of prioritizing assets or provide an analysis tool to allocate funding between disparate assets and activities. This is unacceptable and unrealistic for execution in times of scarce resources. Of the ten documents discussed, only three provide any detail for execution, PDD 63, DoD CIP Plan and the DoD CIP Execution Plan. Together, they guide subordinate execution as follows:

- Focus on the CINC warfighting requirements - specifically those essential to mobilize, deploy and sustain military operations;

- Identify both critical DoD owned and non-DoD owned national defense infrastructure;
- Format the sector plans under the six major topics of: analysis and assessment; remediation; indications and warnings; mitigation; response; and reconstitution.
- Provide a Tier ranking system to prioritize assets.

Although useful, this guidance is not executable by multiple subordinates to achieve a coordinated effort across multiple sectors in an attempt to provide our leaders the information to make intelligent decisions about funding requirements. DoD CIP implies that CINCs will prioritize DoD assets along warfighting requirements, but CINCs do not control the CIP resources in the form of service component budgets. Because CINCs prioritize, and Service Chiefs budget, the allocation decisions must be made at the DoD-level to ensure the warfighting priorities are protected first. The current DoD CIP plan fails to provide a prioritization mechanism, and therefore, our DoD leaders are not equipped to make the necessary strategic decisions. DoD guidance needs to assist our leaders in thinking and acting strategically. Through the NSS and NMS we must have guidance that allows informed decisions to assure the continuity of our most critical and/or most vulnerable assets. If the current DoD CIP guidance is not supplemented with procedures to allow our strategic leaders to prioritize, we will have resigned the protection of our nation's critical infrastructure to the bureaucratic process ensuring a less than optimal solution.

Supplemental DoD guidance should include better use of the terms of protection and assurance. Additionally, the terms of remediation and mitigation should be used consistently. Recommended guidance is:

- Organize analysis and assessment information into a standardized Critical Asset Master List (CAML). Assets should be ranked using the Tier system and potential corrective action to deficiencies identified with the Priority system.
- Sort and use the CAML to rank those most critical assets for assessment studies and/or corrective actions through hardening, redundancy or work-around.
- Require detailed interagency coordination plans for indication and warnings of intentional and/or natural disaster-type disruptions. This is especially critical for assets within the U.S.
- Require detailed Continuity of Operations (COOP) for Tier I and II assets for emergency restoration of that asset or equivalent.

These recommendations should give more definition and/or format to CIP plans, so that CINCS, Components and our DoD leaders can make informed decisions about criticality of assets and priority of funding for the correction of deficiencies.

WORD COUNT = 7,840

ENDNOTES

[1]Kernan Chaisson, "Infrastructure Protection Takes Priority," Journal of Electronic Defense 24 (June 2001): 20.

[2]George W. Bush, "Address to a Joint Session of Congress and the American People," 20 September 2001.

[3]Deputy Secretary of Defense (DSD), The Department of Defense Critical Infrastructure Protection Plan (Washington, D.C., 18 November 1998), 1.

[4]National War College, "The Threat to Critical Infrastructure," 13 February 2001; available from http://www.homelanddefense.org/ELECTIVE5994/NWCSyllabus.htm; Internet; accessed 17 October 2001.

[5]William J. Clinton, WHITE PAPER, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive (PDD) 63 (Washington, D.C.: The White House, 22 May 1998).

[6]DSD, 1.

[7]The roots of CIP policy began in 1995 with Presidential Decision Directive (PDD) 39, which "directed the Attorney General to chair a cabinet committee to assess the vulnerability of the nation's critical infrastructures and recommend measures to protect them. The committee quickly assessed that the potential sources, forms of attack and potential targets was large enough that it required more study than they could provide. It recommended the President issue an Executive Order and create a commission to study how to address the issue. William J. Clinton, U.S. Policy on Counterterrorism: Presidential Decision Directive (PDD) 39 (Washington, D.C.: The White House, 21 June 1995).

[8]Executive Order (EO) 13010, Critical Infrastructure Protection, states that certain national "infrastructures" are critical to the national and economic security of the country.[6] The EO established the President's Commission on Critical Infrastructure Protection (PCCIP) which was chartered to assess threats and vulnerabilities to the nation's infrastructure and to recommend a national policy and strategy for the protection of that infrastructure. The PCCIP submitted its findings in October 1997, but produced neither a useable assessment nor a national policy/strategy. The findings were: 1) that our national infrastructures are vulnerable to both physical and cyber attacks; 2) that there is a lack of awareness of this vulnerability in both the private and public sectors; and 3) that there will need to be a public-private partnership to manage the vulnerabilities. Although the PCCIP did not provide a useable assessment or policy, it did provide the impetus, in May 1998, for Presidential Decision Directive (PDD) 62 and 63, which provides a first-cut at a national policy and organizational structure. William J. Clinton, Executive Order (EO) 13010, Critical Infrastructure Protection (Washington, D.C.: The White House, 15 July 1996).

[9]PDD 62, Combating Terrorism, did not deal specifically with CIP issues, but did strengthen interagency planning through the creation of the Office of the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism. William J. Clinton, Combating Terrorism: Presidential Decision Directive (PDD) 62 (Washington, D.C.: The White House, 22 May 1998).

[10]Robert T. Marsh, Critical Foundations: Protecting America's Infrastructures; The Report of the President's Commission on Critical Infrastructure Protection (Washington, D.C.: The White House, 13 October 1997).

[11]Clinton, PDD 63.

[12]Ibid.

[13]DSD, 1.

[14]Ibid.

[15]CIP is addressed as part of "Protecting the Homeland" in our current National Security Strategy (NSS). Although not well defined in this document, the NSS speaks to our need to protect critical infrastructures associated with information technology, public services, and transportation systems. Specific guidance is to: "protect the ability of state and local governments to maintain order and deliver minimum essential public services while also working with the private sector to ensure the orderly functioning of the economy and the delivery of vital services." William J. Clinton, A National Security Strategy for a Global Age (Washington, D.C.: The White House, December 2001), 24.

[16]Clinton, PDD 63.

[17]John J. Hamre, Departmental of Defense Directive 5160.54 (Washington, D.C.: 20 January 1998), 7.

[18]DSD, 3.

[19]Gaynor, "Critical Infrastructure Protection (CIP); A 21st Century National Security Imperative," briefing slides, United States Pacific Command, December 2000.

[20]DSD, pg 15 and 27.

[21]Richard C. Schaeffer, Jr., DoD Critical Infrastructure Protection Execution Plan (Washington, D.C.: 13 March 2000), 2.

[22]Stephan T. Rippe, Chairman of the Joint Chiefs of Staff Instruction 3110.01C – Joint Strategic Capabilities Plan FY 2000 Interim Guidance (Washington, D.C.: The Joint Staff, 11 May 1999).

[23]Lin Wells, DoD Directive 8590.1 Critical Infrastructure Protection (DRAFT) (Washington, D.C.: 10 August 2001), 2.

[24]DSD, 8.

[25]DSD, 8.

[26]DoD CIP contains an excellent discussion of the meanings of the words assurance and protection, and how the interagency process uses the words interchangeably. Multiple examples and potential applications are discussed. DSD, 7.

[27]James Newport, USPACOM Theater Infrastructure Protection Plan (TIPP) (DRAFT) (Camp Smith, HI: undated), 5.

[28]Schaeffer, 10.

[29]Newport, 3-A-5.

[30]C.W. Fulford, Jr., Chairman of the Joint Chiefs of Staff Instruction 3401.01B – Chairman's Readiness System, (Washington, D.C.: The Joint Staff, 19 June 2000), D-2.

[31]Newport, 10.

[32]Schaeffer, 11.

[33]Philip B. Gove, Webster's, Third New International Dictionary (Springfield, MA: 1965), 1920.

[34]Ibid, 1497.

[35]Schaeffer, 11.

[36]Newport, 9.

[37]Ronald Reagan, Executive Order (EO) 12333, U.S. Intelligence Activities (Washington, D.C.: The White House, 4 December 1981).

[38]Schaeffer, 11.

[39]Newport, 9.

[40]George W. Bush, Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities (Washington, D.C.: The White House, January 2001) 36.

[41]Schaeffer, 11.

[42]Ibid, 11.

GLOSSARY

ASD (C3I). Assistant Secretary of Defense (Command, Control, and Communications).

Assurance. Degree of confidence that a service or commodity will be available and will perform as intended when and where required.

AT/FP. Antiterrorism/Force Protection.

BSA. Balanced Survivability Assessment.

CAAP. Critical Asset Assurance Program.

CAML. Critical Asset Master List.

CBT-RIF. Combating Terrorism – Readiness Initiative Fund

CIA. Central Intelligence Agency.

CIF. CINC Initiative Fund.

CINC. Commander in Chief.

CIP. Critical Infrastructure Protection. The identification, assessment, and assurance of cyber and physical infrastructures that supported mission critical capabilities and requirements, to include the political, economic, technological, and information security environments essential to the execution of the National Military Strategy.

CIPIA. Critical Infrastructure Protection Integration Activity.

CJSCI. Chairman of the Joint Chiefs of Staff Instruction.

CONPLAN. Contingency Plan.

COOP. Continuity of Operations Plans.

Critical Infrastructures. Certain national infrastructures so vital that their incapacity or distraction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures included telecommunications, electronic power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire and rescue), and the continuity of government.

DDR&E. Director of Defense Research and Engineering.

Defense Critical Infrastructures. Those systems and assets essential to mobilize, deploy, and sustain military operations in transition to post-conflict military operations, and whose loss or degradation jeopardize the ability of the Department to execute the National Military Strategy.

DFAS. Defense Finance and Accounting Service

DHRA. Defense Human Resources Agency.

DIA. Defense Intelligence Agency.

DII & C3. Defense Information Infrastructure and Command, Control, and Communications.

DISA. Defense Information Systems Agency.

DIVA. Defense Integrated Vulnerability Assessment.

DLA. Defense Logistics Agency.

DoD. Department of Defense.

DoD Dir. Department of Defense Directive.

DoD (GC). Department of Defense (General Counsel).

DoD CIP. Department of Defense Critical Infrastructure Protection Plan.

DoD CIP EP. Department of Defense Critical Infrastructure Protection Execution Plan.

DoJ. Department of Justice.

DoS. Department of State.

DSD. Deputy Secretary of Defense.

DTRA. Defense Threat Reduction Agency.

EO. Executive Order.

EPA. Environmental Protection Agency.

FEMA. Federal Emergency Management Agency.

FRP. Federal Response Plan.

FY. Fiscal Year.

HHS. Department of Health and Human Services.

HQ. Headquarters.

IAM. INFOSEC Assessment Methodology.

INFOSEC. Information Security.

Infrastructure. The framework of interdependent physical and cyber-based systems comprising identifiable industries, institutions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, the smooth functioning of government and all levels, or society as a whole.

Infrastructure Assurance. The surety of readiness, reliability, and continuity of operations of infrastructures such that they are (1) less vulnerable to disruption or attack; (2) harmed to a lesser degree in the event of a disruption or attack; and (3) can be reality recommended to reestablish vital capabilities.

IPL. Integrated Priority List.

ISR. Intelligence, Surveillance and Reconnaissance.

JTF-CND. Joint Task Force – Computer Network Defense.

JMRR. Joint Monthly Readiness Review.

JSIVA. Joint Staff Integrated Vulnerability Assessment.

JPO-STC. Joint Program Office – Special Technology Countermeasures.

JROC. Joint Readiness Oversight Council.

MACOM. Major Command.

METL. Mission Essential Task List.

MNS. Mission Needs Statement.

NIPC. National Information Protection Center.

NMCC. National Military Command Center.

NMJIC. National Military Joint Intelligence Center.

NMS. National Military Strategy.

NSA-IA. National Security Agency – Information Assurance.

NSS. National Security Strategy.

OASD. Office of the Assistant Secretary of Defense.

OCONUS. Outside the Continental United States.

OPLAN. Operations Plan.

OSTP (R&D). Office of Science Technology (Research and Development).

OUSD (P). Office of the Undersecretary of Defense (Policy).

PCCIP. President's Commission on Critical Infrastructure Protection.

PDD. Presidential Decision Directive.

QDR. Quadrennial Defense Review.

SIOP. Single Integrated Operational Plan.

SOFA. Status of Forces Agreement.

TIPP. Theater Infrastructure Protection Plan.

USACE. United States Army Corps of Engineers.

USA DOMS. United States Army (Director of Military Support).

USPACOM. United States Pacific Command.

USSPACECOM. United States Space Command.

USTRANSCOM. United States Transportation Command.

BIBLIOGRAPHY

Bush, George W. "Address to a Joint Session of Congress and the American People." 20 September 2001.

_____. Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities. Washington, D.C.: The White House, January 2001.

Chaisson, Kernan. "Infrastructure Protection Takes Priority," Journal of Electronic Defense 24 (June 2001): 20.

Clinton, William J. A National Security Strategy for a Global Age. Washington, D.C.: The White House, December 2001.

_____. Executive Order (EO) 13010, Critical Infrastructure Protection. Washington, D.C.: The White House, 15 July 1996.

_____. U.S. Policy on Counterterrorism: Presidential Decision Directive (PDD) 39. Washington, D.C.: The White House, 21 June 1995.

_____. Combating Terrorism: Presidential Decision Directive (PDD) 62. Washington, D.C.: The White House, 22 May 1998.

_____. WHITE PAPER, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive (PDD) 63. Washington, D.C.: The White House, 22 May 1998.

Deputy Secretary of Defense. The Department of Defense Critical Infrastructure Protection Plan. Washington, D.C., 18 November 1998.

Fulford, C.W., Jr. Chairman of the Joint Chiefs of Staff Instruction 3401.01B – Chairman's Readiness System. Washington, D.C.: The Joint Staff, 19 June 2000.

Gaynor. "Critical Infrastructure Protection (CIP); A 21st Century National Security Imperative." Briefing slides. United States Pacific Command, December 2000.

Gove, Philip B. Webster's, Third New International Dictionary. Springfield, MA.,: 1965.

Hamre, John J. Departmental of Defense Directive 5160.54. Washington, D.C.: 20 January 1998.

Marsh, Robert T. Critical Foundations: Protecting America's Infrastructures; The Report of the President's Commission on Critical Infrastructure Protection. Washington, D.C.: The White House, 13 October 1997.

National War College. "The Threat to Critical Infrastructure." 13 February 2001. Available from http://www.homelenddefense.org/ELECTIVE5994/NWCSyllabus.htm. Internet. Accessed 17 October 2001.

Newport, James. USPACOM Theater Infrastructure Protection Plan (TIPP) (DRAFT). Camp Smith, HI: undated.

Reagan, Ronald. Executive Order (EO) 12333, U.S. Intelligence Activities. Washington, D.C.: The White House, 4 December 1981.

Rippe, Stephen T. Chairman of the Joint Chiefs of Staff Instruction 3110.01C – Joint Strategic Capabilities Plan FY 2000 Interim Guidance. Washington, D.C.: The Joint Staff, 11 May 1999.

Schaeffer, Richard C., Jr. DoD Critical Infrastructure Protection Execution Plan. Washington, D.C.: 13 March 2000.

Wells, Lin. DoD Directive 8590.1 Critical Infrastructure Protection (DRAFT). Washington, D.C.: 10 August 2001.